Taking a Pragmatic Approach to Security

Neil Wynne
@neilwynne

#GartnerMSE
We're Spending More on Security …

Total IT Security Spending per Employee, 2014 to 2017

Source: "IT Key Metrics Data 2018: Key IT Security Measures: Multiyear," 11 December 2017 (G00341805)
... Yet More Organizations Suffer Serious Incidents ...

<table>
<thead>
<tr>
<th>Entity</th>
<th>Vertical</th>
<th>Individuals Impacted</th>
<th>Method</th>
<th>Data Sensitivity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yahoo!</td>
<td>Web services</td>
<td>3 billion</td>
<td>Still undisclosed</td>
<td>Names, email addresses, dates of birth, telephone numbers, answers to security questions</td>
</tr>
<tr>
<td>Equifax</td>
<td>Credit risk assessment</td>
<td>147.9 million</td>
<td>Web application vulnerability</td>
<td>Names, Social Security numbers, birth dates, addresses</td>
</tr>
<tr>
<td>eBay</td>
<td>E-commerce</td>
<td>145 million</td>
<td>Credential theft</td>
<td>Names, addresses, dates of birth and encrypted passwords</td>
</tr>
<tr>
<td>Atlanta</td>
<td>Local govt.</td>
<td>Serious disruptions in five of the city's 13 departments</td>
<td>Ransomware</td>
<td>Crippled court system, limited vital communications for infrastructure requests, forced police to file paper reports</td>
</tr>
<tr>
<td>Anthem Blue Cross and Blue Shield</td>
<td>Healthcare</td>
<td>78.8 million</td>
<td>Phishing</td>
<td>Names, Social Security numbers, personal information, health information</td>
</tr>
</tbody>
</table>

All of These Have CISOs and Large Security Teams!
Key Issues

1. When is "good enough" good enough?

2. How can my organization maintain and incrementally enhance its security posture without breaking the bank?
Key Issues

1. When is "good enough" good enough?

2. How can my organization maintain and incrementally enhance its security posture without breaking the bank?
"Good Enough" Security Is an Elusive Goal

- Not reaching "good enough" exposes enterprises to unacceptable risk levels.
- Exceeding "good enough" hurts various aspects of business:
  - Budget
  - IT staff
  - Users
- "Good enough" security is different for everyone and is based on your risk profile:
  - It also changes as your IT environment changes
- Establish an acceptable risk level:
  - Acceptable risk can't be "zero," or else the business stops
Best of Need vs. Best of Breed

As some security functions converge and others commoditize, the balance shifts.

Securability
Managed risks
Known threats
Manageability
Reduced agents, boxes
Reduced consoles
Reduced complexity
Reduced costs

Most secure
Lowest risk
Emerging threats
Multiple point solutions

Convergence
Defending Against an Evolving Threat Landscape

Continuous Adaptive Risk and Trust Assessment

- Attack Protection
  - Prevent/Adaptive Threats
  - Discover/Adaptive Threats
- Access Protection
  - Manage Usage
  - Respond to Incidents
- Posture
  - Continuous Visibility and Assessment
    - Monitor Usage
    - Detect Incidents
    - Adjust Posture
    - Implement Posture
- Policy
  - Continuous
    - Enable Adaptive Responses
  - Adjust Posture
  - Implement Posture
- Defense Posture
  - "Keep Bad Stuff Out"
- Access Posture
  - "Let Good Stuff In"

© 2018 Gartner, Inc. and/or its affiliates. All rights reserved.
Operationalization of Security Can Be a Good Thing

- In more mature and secure environments, overall explicit security activities and expenses decrease as they become subsumed within overall operations. Examples: Firewall management, web antivirus, secure file transfer.

- Where threats are static, security costs can be subsumed within overall operations, leaving budgetary accommodation for protection against new advanced threats.

- Employing secure methodologies in system development, implementation and management processes can lead to overall security cost-efficiencies.

- Explicit security spending also tends to decrease as security capabilities are increasingly bundled into security platforms. Examples: Unified threat management (UTM), secure email gateways (SEG), secure web gateways (SWG), cloud access security brokers (CASB), firewall as a service (FWaaS)
Key Issues

1. When is "good enough" good enough?

2. How can my organization maintain and incrementally enhance its security posture without breaking the bank?
# First, Avoid These Security "Worst Practices"

<table>
<thead>
<tr>
<th></th>
<th>Security Practice</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Shiny new object syndrome</td>
</tr>
<tr>
<td>2</td>
<td>Culture of no</td>
</tr>
<tr>
<td>3</td>
<td>Insufficient focus on users and business requirements</td>
</tr>
<tr>
<td>4</td>
<td>Defense with inadequate depth</td>
</tr>
<tr>
<td>5</td>
<td>Organizational misalignment</td>
</tr>
<tr>
<td>6</td>
<td>Suboptimal branch architecture</td>
</tr>
<tr>
<td>7</td>
<td>Security blind spots</td>
</tr>
<tr>
<td>8</td>
<td>Uncoordinated policy management</td>
</tr>
<tr>
<td>9</td>
<td>Noncompetitive vendor selections</td>
</tr>
<tr>
<td>10</td>
<td>Hazardous network segmentation</td>
</tr>
<tr>
<td>11</td>
<td>Inadequate end-user education</td>
</tr>
<tr>
<td>12</td>
<td>Inadequate security event management</td>
</tr>
</tbody>
</table>
"Simple Things" in Security That You Must Execute Well On

- Vulnerability Management
- Internal Network Segmentation
- Central Log Management
- Application Whitelisting
- Identity and Access Management
- DNS Filtering/Monitoring
- Good Systems Administration

- Backups
- System Hardening
- …

(Yes, the list is bigger than this, but notice there is no "Advanced Persistent …" or "Machine Learning" in here)
Why Aren't We Already Doing These Today?

- **Patching is hard.** Way harder than a lot of security folks think it is:
  - MSEs are challenged with the volume of vulnerabilities identified vs. remediation resources. When you have 100 things, but can only do 10.
  - Vulnerability naming and criticality schemes are a great start, but don't take into account a variable of what "threat actors" are doing.
  - Historically, we haven't had the intelligence on threat actors that we do today. You must have this to understand the true risk of a vulnerability.
  - Security people often forget all the times patches broke things, very badly.

- **Organizational responsibilities and compartmentalization doesn't help.** "Complexity is the enemy of security." The relationships between applications and other systems are complex.
Why Aren't We Already Doing These Today?

- It's an issue of systemic neglect in some cases or it’s just not "cool" enough in others.
- Most marketing and vendors also aren't focused here. Despite their effectiveness, these things are often at the cheaper end of the scale in vendor price lists and end user budgets.
Inventory Your Business Assets Against Your Security Controls

- Identify your most critical data:
  - PII
  - Intellectual property
  - Partner/Customer lists
  - Legal
  - Business-critical applications

- Attach risk ratings
- Look for gaps
### There's a Lot of Security Stuff You Can Buy …

<table>
<thead>
<tr>
<th>Keep the Bad Guys Out</th>
<th>Let the Good Guys In</th>
<th>Keep the Wheels On</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Threat-Facing Technologies</strong></td>
<td><strong>Identity and Access Management</strong></td>
<td><strong>Business Continuity and Governance</strong></td>
</tr>
<tr>
<td>▪ Firewall as a Service (FWaaS)</td>
<td>▪ Cloud Multifactor Authentication (MFA)</td>
<td>▪ Disaster Recovery as a Service (DRaaS)</td>
</tr>
<tr>
<td>▪ Network Sandboxing</td>
<td>▪ Privileged Access Management (PAM)</td>
<td>▪ IT Vendor Risk Management</td>
</tr>
<tr>
<td>▪ Cloud Access Security Brokers (CASBs)</td>
<td>▪ Managed Security Service Providers (MSSPs)</td>
<td></td>
</tr>
<tr>
<td>▪ Managed Detection and Response (MDR)</td>
<td>▪ Managed Detection and Response (MDR)</td>
<td></td>
</tr>
<tr>
<td>▪ Security Information and Event Management (SIEM)</td>
<td>▪ Security Information and Event Management (SIEM)</td>
<td></td>
</tr>
<tr>
<td>▪ Remote Browser Isolation</td>
<td>▪ Managed Detection and Response (MDR)</td>
<td></td>
</tr>
</tbody>
</table>

© 2018 Gartner, Inc. and/or its affiliates. All rights reserved.
… So How Do You Evaluate and Make Sense of It All?

Security Playlist Innovation Evaluator

- Size of bubble indicates Potential MSE Value
- Low Operational Risk (Best)
  - MSS
  - Threat Sandboxing
  - FWaaS
  - MDR
- High Operational Risk (Worst)
  - Remote Browser Isolation
  - CASB
  - IDaaS
  - PAM
  - MFA

Low Current MSE Applicability

High Current MSE Applicability

ID: 355786

© 2018 Gartner, Inc. and/or its affiliates. All rights reserved.
Use the Cloud to Secure and Manage the Cloud

✓ Maintain data center and hardware security: All public cloud types
✓ Manage identities and authorizations: IDaaS
✓ Control application vulnerabilities: Application security as a service
✓ Fight malware:
  – Scan data in cloud before it gets on your endpoints
  – Backup data to cloud where it is protected from ransomware
  – Use cloud-based applications instead of personal productivity files

Leverage the security expertise and capabilities of cloud-based security products
Resource-Strapped MSEs Should Consider Managed Security Services as Opposed to "Do It Yourself"

- Managed firewalls
- Managed intrusion detection and prevention systems
- Distributed denial of service (DDoS) protection
- Managed secure email gateways
- Reporting associated with monitored and managed devices and incident response

- Managed vulnerability scanning of networks, servers, databases and applications
- Vulnerability and threat notification services
- Log management and analysis
- Managed secure web gateways
- Security information and event management (SIEM)

MSSPs are responsible for managing and monitoring; You are responsible for reacting to events the MSSP reports.
### How Clients Are Using Managed Security Services

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Engagement Theme</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSSP as a check box</td>
<td>&quot;We need to do something about security.&quot;</td>
</tr>
<tr>
<td>MSSP as an outsourced provider</td>
<td>&quot;We want you to take care of our security; please take security off our hands.&quot;</td>
</tr>
<tr>
<td>MSSP as an integrated partner</td>
<td>&quot;Please detect threats for us and manage our devices.&quot;</td>
</tr>
<tr>
<td>MSSP as a cover for a specific gap</td>
<td>&quot;We can do this task well ourselves, but we think you can do it less expensively.&quot;</td>
</tr>
</tbody>
</table>

A minimum of eight to 12 security analysts are required for 24/7 monitoring; an unrealistic objective for most MSEs.
The Rise of Managed Detection and Response (MDR)

Now

Advanced MSS

"Basic" MSS

MSSP

MDR

Next 24 Months

Advanced MSS/MDR

"Basic" MSS

MSSP

MDR
Where MDR Differs From MSS

✓ Scope
✓ Technology Dependence
✓ Quality of Analytics
✓ Access to Analysts
✓ Actionable Advice on Incident Response (or Even Doing Containment for the Customer)
✓ SLAs
✓ Ability to Remediate (or Suggest Remediation)
Recommendations

✓ Doing the simple things well means the more difficult things in IT security are easier. Complexity is the enemy of security.

✓ Start to seriously examine how to leverage your security spending with multifunction platforms.

✓ Demand a secure development life cycle and "built-in" security for IT components.

✓ Constantly re-evaluate your risk tolerance and your "good enough" security comfort level.

✓ Investigate emerging security services.
Recommended Gartner Research

- **Taking a Pragmatic Approach to Infrastructure Security for Midsize Enterprises**
  Claudio Neiva, Adam Hils and Prateek Bhajanka (G00333594)

- **Magic Quadrant for Managed Security Services, Worldwide**
  Toby Bussa, Kelly M. Kavanagh, Sid Deshpande and Pete Shoard (G00325535)

- **Market Guide for Managed Detection and Response Services**
  Toby Bussa, Craig Lawson, Kelly M. Kavanagh and Sid Deshpande (G00308991)

- **Avoid These "Dirty Dozen" Network Security Worst Practices**
  Andrew Lerner and Jeremy D'Hoinne (G00271440)